

There are several key HIPAA related pieces of news:

1) As discussed in our HIPAA Workgroup Meeting on Monday, the Office of HIPAA Implementation (OHI) is getting established and starting to initiate steps to fulfill their legislated business processes. A DRAFT of their Initial Assessment for state departments is available for comment on the HIPAA Website at

http://www.dmh.cahwnet.gov/hipaa2001/docs/agenda/hipaa_ohi_draft.pdf

Please pass your comments to Therese Hart at thart@OHI.ca.gov by Friday, October 26.

2) Evaluators for the HIPAA Master Services Agreement are needed. Evaluators can be either State or County employees. Your help on the evaluations may take about a week. If you are able to participate in this valuable and critical task, please contact Tara Naisbitt at (916) 255-6004 or email her at Tnaisbit@dhs.ca.gov. Please respond directly to Tara by cob Friday, October 26. (Please see the first e-new item below.)

3) A very special project has been formed to compare HIPAA to CA Privacy Law. The objective of the group is to develop a comprehensive matrix-format comparison of the HIPAA Privacy Rule to existing California and federal privacy laws. To participate in this very timely project please contact David Smith at dsmithcc@co.san-diego.ca.us or Cheri Huber at CHUBER@co.napa.ca.us.

4) At the CMS (formerly HCFA) website, there are some excellent White Papers available, including one titled "Are You A Covered Entity?". Please see the e-news item titled: "CMS Website and Great information".

Please be sure to note that in some cases the information presented may be the opinion of the original author. We need to be sure to view it in the context of our own organizations and environment. In some cases you may need legal opinions and/or decision documentation when interpreting the rules.

Many thanks to all who contributed to this information!!!

Have a great day!!!

Ken

Items included below are:

- Evaluators for the HIPAA Master Services Agreement.

- CMS Website and Great information

- Some Providers Exempt from Privacy Rule

- Disclaimers

- [hipaalive] HIPAA Regs apply to.....

- [hipaalive] AHIMA excerpt

- [hipaalive] SECURITY FOR CAPITATED

- [hipaalive] TCS: 837 Claims Size

- [hipaalert] HIPAAAlert-lite 10/23/01 (ATTACHED)

WEDI SNIP Synopsis (ATTACHED)
HIPAA Implementation Newsletter - Issue #20 - October 19, 2001
(ATTACHED)

>>> "Gelein, Judy (DHS-PSD-OMPS)" <JGelein@dhs.ca.gov> 10/23/01
2:47:20 PM >>>

The California Department of General Services is seeking volunteers to assist in performing evaluations on incoming bids for the HIPAA Master Services Agreement. Our understanding is that if there are twenty volunteers, it should not take more than 1 week of fulltime evaluation time. We are requesting that county staff participate in this evaluation. It is anticipated that staff would be needed during the second week of November, in Sacramento. If you are able to participate, please contact Tara Naisbitt at (916) 255-6004 or email her at Tnaisbit@dhs.ca.gov. Please respond directly to Tara by cob Friday October 26. Thank you.

Judy Gelein, Chief
DHS - Office of HIPAA Compliance

***** CMS Website and Great information

Medicaid HIPAA Administrative Simplification
<http://www.hcfa.gov/medicaid/hipaa/admsimp/>

Federal DHHS's FAQ's are at: <http://aspe.hhs.gov/admsimp/qdate01.htm>

HCFA (CMS) White Papers at:
<http://www.hcfa.gov/medicaid/hipaa/admsimp/whitepap.htm>

Some of the White Papers are:

Vol. 2, Map 1 ARE YOU A COVERED ENTITY?... The paper covers the following subjects: How to tell if you and your data trading partners are Covered Entities; How to draw the boundary for your program, identifying the Covered Entities, covered standard transactions, and covered business cases within your domain and those that are beyond the pale; and Approaches for resolving the tough issues and answering the complex questions that require interpretation.

Vol. 1, Map 5 GETTING ORGANIZED FOR HIPAA States Provide Trail Markers and the Best Approach Up the South Face. The first component of the good practices package is the leadership role of state government. The Single State Agency for Medicaid is defined differently by each state. A few are stand-alone organizations but most are part of a larger health care human services, or combined agency. HIPAA crosses over the boundaries of State agencies. Therefore, the higher the level of authority for implementing HIPAA, the greater the opportunity for coordination and cooperation across all affected agencies, departments, division, et al.

Vol. 1, Map 4 DATA CONTENT AND CODE SETS: THE DEVIL IS IN THE DETAILS The essence of the HIPAA Administrative Simplification Transactions and Code Sets Final Rule is that we will all benefit from the implementation of common standards for data transmission and the adoption of national standards for the health care information that we communicate. This paper summarizes key points about data content requirements, the problem of local codes, what you need to do to be compliant, the change processes, and the ultimate benefits.

Vol. 1, Map 3 THE ROLE OF TRANSLATORS The role of the translator The role of the translator in meeting the electronic data interchange (EDI) requirements of HIPAA. It examines why it may be needed, what it can do, what the installation alternatives are and some criteria for product or vendor selection.

Vol. 1, Map 2 PREVIEW OF THE MEDICAID HIPAA COMPLIANT CONCEPT MODEL (MHCCM) How CMS's MHCCM can help your state stay on the road to success. The MHCCM demonstrates how HIPAA impacts the Medicaid Enterprise and provides practical tools to help you determine the best course of action based on your circumstance.

Vol. 1, Map 1 HOW HIPAA IS RESHAPING THE WAY WE DO BUSINESS: The Benefits and Challenges of Implementing the Administrative Simplification Standards

***** Disclaimers

*** This is HIPAAlive! From Phoenix Health Systems ***

You should take what this attorney says very seriously. Lawyers do not like competition from non-lawyers. It is extremely important that you protect yourself by making it clear that you are not offering legal advice as part of your consulting services. For example, this is the disclaimer that I include in all of the PrivaPlan materials:

"The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Users should consult their own legal or other professional advisors for individualized guidance regarding the application of the law to their particular situations, and in connection with other compliance-related concerns."

I would also strongly recommend that you have your consulting contracts and other materials reviewed by your own lawyer to ensure that your personal exposure is minimized. Good luck!

Bye for now -- Harry

Harry E. Smith, CISSP
Timberline Technologies LLC

***** Some Providers Exempt from Privacy Rule *****
*** This is HIPAAlive! From Phoenix Health Systems ***

The following appears of relevance to the issue under discussion:

<http://www.healthdatamanagement.com/html/supplements/himss/HimssNewsStory.cfm?DID=4544>

Some Providers Exempt from Privacy Rule

(February 09, 2001) Large numbers of health care providers are not required to comply with the final medical privacy rule because of a quirk in the rule's definitions. The rule is authorized under the administrative simplification provisions of the Health Insurance Portability and Accountability Act. Providers covered under the provisions include only those electronically transmitting and receiving claims and related transactions. HIPAA requires the adoption of national standard formats for electronic transactions but does not require the use of electronic transactions. As a result, providers that do not electronically transmit or receive claims-related transactions are not covered entities under the privacy rule, according to William Braithwaite, senior advisor on health information policy at the Department of Health and Human Services. He spoke at several educational sessions of this week's 2001 HIMSS Conference and Exhibition in New Orleans.

Several major segments of the provider community, including dentists and mental health professionals, lag behind in the adoption of electronic data interchange to conduct administrative and financial transactions. While paper-based providers are not covered under the privacy rule, they still may face legal liability if they do not comply with the rule, according to several industry experts. That's because they could be sued under state statutes requiring providers to comply with certain "standards of care." The privacy rule is setting such standards of care for the protection of patient confidentiality, experts say. They suggest paper-based providers seek legal counsel to determine their liability under the new privacy rule.

***** [hipaalive] HIPAA Regs apply to.....

*** This is HIPAAlive! From Phoenix Health Systems ***

The regs are very clear: they only apply to "covered entities." And there is only one definition of covered entity for all the regs - TCS, Security and Privacy: (1) a health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered for which HIPAA establishes a

standard.

The confusion that stems from the proposed privacy rules is this: The proposed rules only applied to information that was electronically stored or transmitted by a covered entity. So the PHI had to be both electronic (or once electronic -- the rule applied to print-outs) AND in the custody of a covered entity.

The final rule applies to all PHI (in whatever medium: paper, electrons, human voice, jell-o, sky writing, etc.) that is in the possession of a covered entity. But-- you still have to be a covered entity for it to apply. And, as I said, there's only ONE definition of covered entity:

"Covered Entity means (1) a health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. " Section 160.103.

Also, Section 160.102 says, "except as otherwise provided, the standards, requirements and implementation specifications adopted under this subchapter apply to the following entities: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits information in electronic form in connection with a transaction covered by this subchapter."

For those of you reading along in the federal register, Sections 160.102 and 160.103 are included in Part 160 of *Subchapter* C - Administrative Data Standards and Related Requirements. (See FR of 12/28/2000, pg. 82797.) If you read on further you will find on pg. 82802 that a new Part 164 is added to the same subchapter. As we all know, Part 164 is our beloved privacy rule. Same subchapter, same definition of covered entity.

Part 164.104 (Applicability) of the privacy regulations further states clearly that "except as otherwise provided, the standards, requirements and implementation specifications adopted under this subchapter apply to the following entities: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits information in electronic form in connection with a transaction referred to in section 1173(a)(1) of the Act (meaning HIPAA)"

Section 1173(a)(1) of the Act is the legal authority for the Secretary to adopt transaction standards.

Speaking of the Act, Section 1172(a) of the Act says " Applicability.--Any standard adopted under this part shall apply, in whole or in part, to the following persons: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in

electronic form in connection with a transaction referred to in section 1173(a)(1).

Finally, section 164.500(a) of the regulation says "Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart [that is Subpart E - Privacy of Individually Identifiable Health Information, of Part 164] apply to covered entities with respect to protected health information." And remember, the definition of "covered entity" as found in section 160.103 applies to the whole subchapter, of which subpart E of Part 164 is a part.

I've read through the regulations too often to want to remember, and I have yet to encounter an exception which extends the privacy rule to something that is not a covered entity. And there is only one definition of covered entity for all of HIPAA.

Paper-only providers, if any still exist, are not subject to any of HIPAA: TCS, Security or Privacy.

Have a happy weekend.
Bill MacBain
MacBain & MacBain, LLC
wam@MacBainandMacBain.com

***** [hipaalive] AHIMA excerpt

*** This is HIPAALive! From Phoenix Health Systems ***

This is an excerpt from the current AHIMA Conference

Former CMS security chief: HIPAA standards promote good practice

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) security standards are based upon good business practices, John Parmigiani, former Centers for Medicare and Medicaid Services security chair for HIPAA, emphasized at his presentation yesterday at the American Health Information

Management Association national convention. The standards, which require providers, as well as insurance companies and clearinghouses, to establish administrative, technical, and physical safeguards to protect patient data, are still in the proposal stage. But finalization is due this year or early 2002. Smart health information management (HIM) and information technology

professionals are assessing the standards now to get a jump on compliance. "The standards are reasonable and already in use by other industries, such as

automotive and finance," Parmigiani said. He added that they "tell you what

to do, now how to do it," and are scalable. They are also technology neutral, meaning that particular vendors are not endorsed in the rule. Twenty-four standards make up the rule. (HIPAA's privacy rule consists of 58 standards.) The bulk (12) are administrative, which designate roles and responsibilities and require awareness, training, and risk assessments. Six of the standards are physical and require "common sense" approaches to physically protecting patient information, such as locking doors and escorting visitors. The rest are technical requirements. Examples are audit trails and automatic log-offs. "The emphasis on this rule was trying to do things that make sense," Parmigiani added. He said that while HIPAA's proposed privacy rule triggered 250,000 comments from the public, only 2,350 comments were submitted in response to the security rule, making it the least controversial of the HIPAA regulations proposed to date. Still, compliance with HIPAA's security rule is not going to be easy. It will require multidisciplinary involvement and buy-in from the very top. The rule affects everyone who has access to health information, including management, clinicians, volunteers, HIM staff, vendors, and contractors. "The rule requires a change of culture," Parmigiani said. "And culture changes take time." Security breaches will result in fines, and, perhaps, even worse: bad publicity. Parmigiani asked the audience

to ponder the consequences of a breach reported on the news program, "60 Minutes." "Good security can reduce liabilities," he said. "And should not impede patient care." So how do you get started? Parmigiani provided five tasks that organizations could be taking now to prepare for the security regulations: 1. Assign responsibility. Who is going to lead your organization's information security efforts? Where does the buck stop? 2. Create a HIPAA team. Be sure to involve staff from all disciplines, since information security impacts everyone. 3. Do a readiness assessment. If the security regulations were enforceable today, would you be in compliance? In this process, identify those areas that need attention. 4. Review and update existing policies and procedures. Watch out for noncompliance with existing policies. (A policy does no good if it sits on a shelf and no one uses it," Parmigiani added. Also, talk to business partners and system vendors. Make quick fixes now and address "low-hanging fruit." 5. Provide training, education, and awareness. This has to be documented and ongoing. Parmigiani

explained the difference between the three: "Training is showing, educating is telling, and awareness is constantly reminding." Editor's note: HIPAA security regulations will be enforceable 26 months after the rule is finalized. To download the proposed security regulation. Hope you enjoy this.

Allan Tobias, MD. JD
Healthcare Consulting & Law
(925) 935-5517
FAX (925) 932-2741
E-MAIL altoby@aol.com

***** [hipaalive] SECURITY FOR CAPITATED

*** This is HIPAALive! From Phoenix Health Systems ***

According to HIPAA's claim transaction standard "if there is no direct claim, because the reimbursement contract is based on a mechanism other than

charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care." Section 162.1101(b). Since your state law is contrary to this, and none of the preemption exceptions seems to apply, HIPAA will pre-empt the state law and these encounter reports will be considered HIPAA claims. If providers report to you electronically, they must use the 837. And you must be prepared to accept it and process it without delay. Since you are a health plan, you must also be prepared to conduct the other transactions for which HIPAA has set a standard, either directly or through a clearinghouse. If you require providers, employers, or other entities to go through a clearinghouse in order to transmit standard transactions to you, or receive standard transactions from you, you will have to pay the cost of using the clearinghouse.

Bill MacBain

MacBain & MacBain, LLC

wam@MacBainandMacBain.com

***** [hipaalive] TCS: 837 Claims

Size *****

*** This is HIPAALive! From Phoenix Health Systems ***

It is in the 275 where you could run into problems. The BIN segment will contain the entire HL7 message. According to X12 syntax, BIN02 can be up to 999,999,999,999 bytes long, although the Standard note recommends that the BIN02 not be larger than 64 MB. And you need to add up to 24 bytes of additional information between the BIN tag, delimiters, and BIN01.

Just to reassure you, none of the proposed attachments for the 275 carry images in them, so we don't expect very large BIN segments. I suspect 16-32-64 KB will be a practical maximum size.

I know you were specifically asking about the 837, but you seem to be sizing some buffer in a program, so you ought to know about the 275 also.

Kepa Zubeldia

Claredi